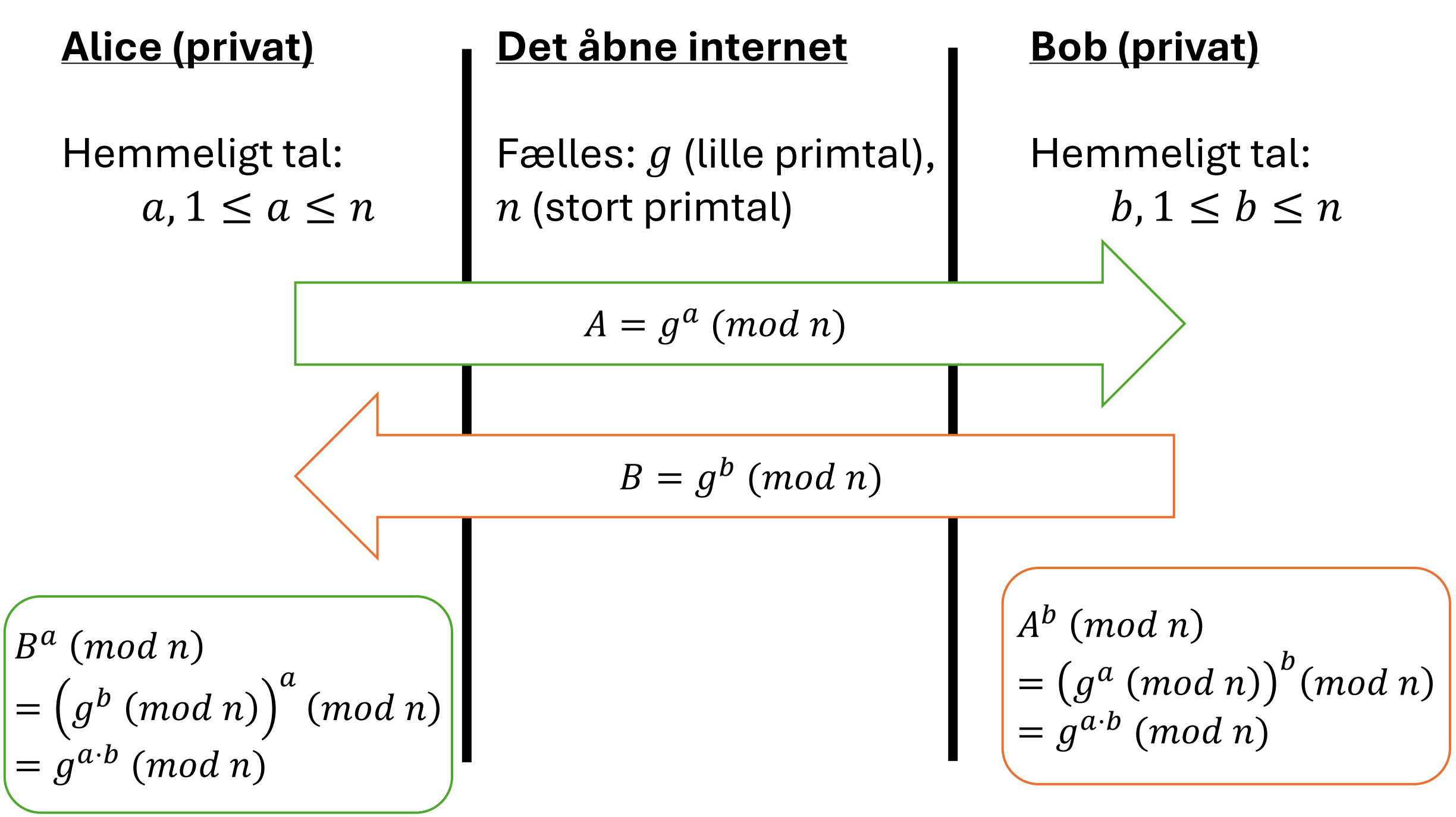
Diffie-Hellman key exchange

Hvordan virker det?


Alice (privat)
Det åbne internet
Bob (privat)
Hemmeligt tal:
$a, 1 \leq a \leq n$
Fælles: g (lille primtal),
n (stort primtal)
Hemmeligt tal:
$b, 1 \leq b \leq n$
$A = g^a \ (mod\ n)$
$B = g^b \ (mod\ n)$
$B^a \ (mod\ n)$
$= \left(g^b \ (mod\ n)\right)^a \ (mod\ n)$
$= g^{a \cdot b} \ (mod\ n)$
$A^b \ (mod\ n)$
$= \left(g^a \ (mod\ n)\right)^b (mod\ n)$
$= g^{a \cdot b} \ (mod\ n)$

Øvelse: Hemmelige beskeder!

- Vi laver 2-mands grupper på Lectio
  (og I må ikke sidde ved siden af hinanden)

- Elevfeedback i Lectio bruges til at udveksle offentlige nøgler og krypterede beskeder. Dvs. til start udveksler I følgende offentligt:
  - g (lille primtal), n (stort primtal)
  - "Alice" sender $A = g^a \ (mod\ n)$
  - "Bob" sender $B = g^b \ (mod\ n)$

HUSK!
a og b er top secret!

- I bruger den beregnede nøgle og laver AES kryptering her: https://encode-decode.com/aes256-encrypt-online/

- De krypterede beskeder sender I via elevfeedback og dekrypterer på samme side, hvor I krypterede.

Øvelse: Hemmelige beskeder!

- Vi laver 2-mands grupper på Lectio
  (og I må ikke sidde ved siden af hinanden)

- Elevfeedback i Lectio bruges til … Dvs. til start udveksler I fø…
  - g (lille …
  - ”Alic…
  - ”Bob…

- I bruger de… decode.com…

- De krypterede … I via elevfeedback og dekrypterer på samme side, hvor I krypterede.

Svin din lærer til, uden at hun opdager det!!